OFFICE OF THE CITY PROSECUTOR

CITY OF LONG BEACH

333 W. Ocean Blvd., 2nd Floor | Long Beach, CA 90802 | (562) 570-5600 FAX (562) 570-7140

THOMAS M. REEVES
CITY PROSECUTOR

CITY PROSECUTOR ALERT
MAY 2006

COMPUTER SAFETY TIPS

Dear Friend,

As the number of computer users continues to increase, so does the number of potential victims of identity theft. In addition to personal computers, a growing number of people use public computers at libraries, Internet cafes, airports and coffee shops to check their email or the status of personal accounts, potentially compromising their personal information. Below are five tips to help protect you against identity theft when using public computers.

1. Don't save your login information: Always logout of Web sites by pressing *logout* on the site. Closing the browser window or typing in another address is not sufficient. Logging out will help keep other users from accessing your information. Many programs (especially instant messenger programs) include automatic login features that will save your username and password. Be sure to disable this option so that no one accidentally (or on purpose) logs in as you.

2. Don't leave the computer unattended with sensitive information on the screen: If you have to leave the public computer for any amount of time, logout of all programs and close all windows that may include sensitive information.

3. Erase your tracks: Web browsers such as Internet Explorer keep a record of your passwords and every page you visit - even after you've closed them (and logged out). When you have finished using a public computer, you should delete all the temporary files and your Internet history.

4. Watch for over-the-shoulder snoops: Because there's so much in the news about how hackers can digitally sneak into your personal files, people sometimes forget about the old fashioned version of snooping. When using a public computer, be on the look out for thieves who collect information by looking over your shoulder or watching as you enter sensitive passwords.

5. Don't enter sensitive information into a public computer: The measures listed above will provide some protection against casual hackers who use a public computer after you have. However, a sophisticated thief may have installed software on the public computer that will record every keystroke and then e-mail that information back to the thief. In that case, it doesn't matter if you haven't saved your information or if you've erased your tracks. Thieves will still have access to this information. That is why you should exercise caution when entering sensitive information into a public computer.

For questions about this letter, or for additional information on the City Prosecutor's Office, please call my Director of Community Relations Noel Hacegaba at (562) 570-5828.

Regards,

Tom

TOM REEVES

Watch City Prosecutor Tom Reeves on the award-winning program
Letter of the Law *Thursdays on Cable Channel 8 at 5:30 PM.*